PATENT ABSTRACTS OF JAPAN

(11)Publication number : 62-012227
(43)Date of publication of application : 21.01.1987

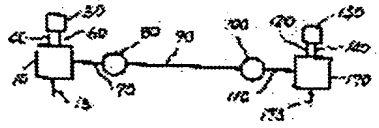
(51)Int.CI. H04L 9/00

(21)Application number : 60-150162
(22)Date of filing : 10.07.1985

(71)Applicant : HITACHI LTD
(72)Inventor : YAGI HIROYUKI
TAKARAGI KAZUO
SASAKI RYOICHI

(54) PRIVACY COMMUNICATION SYSTEM

(57)Abstract:
PURPOSE: To obtain a privacy communication system possible for privacy information with an optimum state by selecting a means of ciphering and decoding so as to attain a proper transmission speed and strength of ciphering.
CONSTITUTION: Data terminal equipments 10, 170 are located at a contact between the data communication system and the user, the information is sent through signal transmission cables 70, 110 and inputted to data line terminators 80, 100. In matching with the sent information, a flag sequence, a bit pattern and a bit inserted location are selected and an optimum transmission speed and intensity of ciphering are selected. Memories 50, 130 are added to the data terminal devices to add a function of addition/deletion of a start/end flag sequence, processing not mixing the flag sequence and other bit pattern in the frame and selecting the said processing in matching with the priority of transmission speed or priority of intensity of ciphering to the data terminal devices 10, 170.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭62－12227

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和62年(1987)1月21日
H 04 L 9/00		Z－7240－5K	

審査請求　未請求　発明の数 1　（全6頁）

⑤4発明の名称　秘匿通信方式

⑳特　願　昭60－150162
㉒出　願　昭60(1985)7月10日

⑦2発明者　八木　郭之　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
⑦2発明者　宝木　和夫　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
⑦2発明者　佐々木　良一　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
⑦1出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
⑦4代理人　弁理士　小川　勝男　外1名

明　細　書

発明の名称　秘匿通信方式

特許請求の範囲

1．データ送信装置，データ受信装置及びデータ伝送媒体から成る通信回線において、暗号化及び、復号化する手段を選択し、最適な手段により、情報の秘匿を行うことを特徴とする秘匿通信方式。

2．暗号化、及び復号化する手段の選択を暗号キーを変えることにより行うことを特徴とする特許請求の範囲第1項記載の秘匿通信方式。

発明の詳細な説明

〔発明の利用分野〕

本発明は、通信回線において、データの傍受，改竄を防止するための、秘匿通信方式に関する。

〔発明の背景〕

従来の秘匿通信方式としては、伝送速度，暗号強度を選択するものは、見当らない。

〔発明の目的〕

本発明は、伝送速度及び、暗号強度を最適な状態にしながら情報の秘匿を行うことが可能な秘匿通信方式を実現することにある。

〔発明の概要〕

本発明では、上記目的を、達成するために、適切な伝送速度、及び暗号強度となるように暗号化及び復号化の手段を選択して情報の秘匿を行うものである。

〔発明の実施例〕

第1図は本発明による秘匿通信方式の一実施例を示したものである。

まず初めに、第1図において従来の通信回線と同様な基本的構成及び、動作について簡単に説明する。データ端末装置10，170はデータ通信システムと利用者との接点に位置する装置であり、情報の入出力を行う計算機，端末装置等である。その情報は、信号伝送用ケーブル70，110により、伝送され、データ回線終端装置80，100に入力される。データ回線終端装置80，100では、データ端末装置10，170間の距離がはなれている等の理由により、データ端末装置から

の信号を変換して伝送する働きをもつている。データ端末装置により変換された信号は、信号伝送用ケーブル９０により伝送され通信が成立される。

本発明は、ＩＳＯ（インタナショナル・オーガンゼーション・フオー・スタンダーダイゼーション：International Organization for Standardization）のＯＳＩ（オープン・システム・インタコネクション：Open System Interconnection）参照モデルの中のデータリンク層に相当する伝送手順において、透過性が保証されているものであれば、ほとんどの通信回線に適用可能である。しかしながら、ここでは第１図に示した通信回線をもとに、データ端末装置１０，１７０が計算機、信号伝送用ケーブル７０，110がベースバンド伝送、データ回線終端装置８０，１００がモデム、信号伝送用ケーブル９０がブロードバンド伝送である場合を例に説明する。

また、ネットワークアーキテクチヤとしては、前記ＩＳＯのＯＳＩ参照モデルに準拠している場合を例にとり、秘匿を実現するために、データリンク層としては、HDLC手順に新しい機能を追加したものを採用した場合について説明する。

本実施例では、第２図に示したフレームフオーマットにより情報の伝送が行われ、フラグシーケンス２００：８ビット，フラグ制御シーケンス２１０：８ビット，アドレスシーケンス２２０：８ビット，制御シーケンス２３０：８ビット，情報シーケンス２４０：任意ビット，フレームチエックシーケンス２５０：１６ビット，フラグシーケンス２６０：８ビットより構成される。

ここで、上記フレームフオーマットより、フラグ制御シーケンス２１０を取り除くことにより、HDLC手順の基本的なフレームフオーマットと同じになることがわかる。したがつて、フラグシーケンス以外の各シーケンスの機能はHDLC手順における機能と同様である。

次に本実施例の説明を容易に行うためにHDLC手順におけるフレームの開始と終了を検出する方法について記述する。

HDLC手順におけるフレームフオーマットの中で、フラグシーケンス２００，２６０は、各フレームの開始と終了を示すシーケンスであり、'01111110'というビットパターンで表わされている。従つて'01111110'というビットパターンを監視するだけで、フレームの開始と終了を検出することが可能となる。ただし、フラグシーケンス以外の場所にも、'0111110'というビットパターンが出現する可能性があるため、そのビットパターンをフラグシーケンスと誤つて検出しないように、受信側においてフラグシーケンス以外の場所に'1'ビットが連続して五つ表われた場合は、次に'0'ビットを挿入することによりフラグシーケンスとの混同を防いでいる。また、フレームの開始と終了を検出したあとで伝送された情報を読み取る場合は、'1'ビットが連続して五つあらわれた後の'0'ビットを取り除くことにより元の状態に戻すことができる。

本実施例では、フラグシーケンスのビットパターンとフラグシーケンスと混同しないために挿入するビットパターン及びその挿入位置を各フレームごとに変更することによりデータの秘匿を行い、さらに、伝送する情報にあわせて、フラグシーケンス，ビットパターン及びビット挿入箇所を選び、最適な伝送速度，暗号強度を選択するものである。

次に、具体的な装置を例に説明を行う。第１図に示すように、従来の通信回線における、データ端末装置に、メモリ５０，１３０を追加し、第３図，第４図に示すような、開始・終了フラグシーケンスの追加，削除及びフラグシーケンスとフレーム内の他のビットパターンとを混同しないための処置と、以上の処置を伝送速度優先、又は暗号強度優先のそれぞれの要求にあわせて選択する機能を、データ端末装置１０，１７０に追加することによつて行われる。

ここでは、理解を容易にするために、第１図においてデータ端末装置１０から送信を行い、データ端末装置１７０で受信する場合についてのみ説明をおこなうが、逆の場合であつても同様に通信が可能であり、従つて全二重通信への適用も可能である。

初めに、データを伝送する場合であるが、この場合は従来のデータ端末装置の機能に第３図に示したデータ処理フローを追加することにより行われる。

まず、データが送信されることによつてスタート（START)する。

ブロック３００では、最初のフレームのみ開始フラグシーケンス'01111110'の伝送を行う。

ブロック３１０では、伝送速度優先、又は暗号強度優先の要求信号１５（データ端末装置１７０から情報を伝送する場合は１７５）に従い、伝送する情報にあつたフラグ制御番号を選択する。

本実施例では、各フレーム単位で要求信号１５に従つて、伝送速度、及び暗号強度の優先度を変えることが可能である。

ブロック３２０では、メモリ５０からフラグ制御番号に対応したフラグシーケンス，ビット挿入箇所，ビットパターンを入力する。

尚、メモリ５０，１３０内には、第５図に示すような、各フラグ制御番号に対応したフラグシーケンス，ビット挿入箇所（矢印），ビットパターンのそれぞれが記憶されているものとする。

なお、第５図の左側ビットより伝送されるものとする。

ブロック３３０では、フラグ制御番号に関する情報であるフラグ制御シーケンスを伝送する。このときフラグ制御番号を暗号の形で伝送することにより、データの傍受及び改竄をより一層困難にすることが可能である。

ブロック３４０では、フラグシーケンス以外の部分にビット挿入箇所が存在するか否かの判定を行う。ビット挿入箇所が存在する場合は、ブロック３５０により、ビット挿入箇所に対応するビットパターンを入力する。

ブロック３６０では、フラグシーケンス以外の総ての情報を伝送する。

ブロック３７０では、ブロック３２０でメモリより入力したフラグシーケンスを終了フラグシーケンスとして伝送する。

ブロック３８０では、データ送信を終了するか否かを判定して、もし終了するのであれば次のフレームの伝送は行わずＥＮＤとなる。更にデータ伝送を続行する場合は、ブロック３９０により終了フラグシーケンスと同じシーケンスが開始フラグシーケンスとして伝送される。この場合データが連続して伝送されるのであれば開始又は終了フラグシーケンスのどちらか一方を省略してもかまわない。

次に、データ端末装置１７０で行われている、受信方法について説明する。

受信の場合は、第４図に示すごとくデータの受信と共にSTART し、最初のフレームのみ、ブロック４００により開始フラグシーケンス'01111110'の検出が行われる。

ブロック４１０では、開始フラグシーケンスの除去が行われる。

ブロック４２０では、フラグ制御シーケンスの検出を行いフラグ制御番号を求める。

ブロック４３０では、メモリ１３０よりフラグ制御番号に対応した、フラグシーケンス，ビット挿入箇所，ビットパターンの入力を行う。ここで、メモリ５０，１３０には、同じデータが入力されているものとする。

ブロック４４０では、終了フラグシーケンスが検出されたか、否かの判定を行う。

終了フラグシーケンスが検出されていなければ、ブロック４６０により、ビット挿入箇所が検出されたか、否かの判定を行い、検出されていればブロック４７０により、その次にくるビットパターン（ブロック４３０でメモリから入力したもの）の除去を行う。

ブロック４６０によりビット挿入箇所の検出が行われなかつた場合又は、ブロック４７０での処理が終了した後は、再びブロック４４０により、終了フラグシーケンス検出の判定が行われる。

終了フラグシーケンスが検出された場合は、ブロック４５０により終了フラグシーケンスの除去が行われる。

ブロック４８０では、データ送信終了か、否かの判定が行われ、終了するのであればＥＮＤとな

る。

更にデータ送信が続行されるのであれば、ブロック４９０により開始フラグシーケンスの検出が行われ、再びブロック４１０に処理がうつされる。

以上の方法により、伝送速度優先、又は暗号強度優先の要求にしたがつた、秘匿通信方式を実現することが可能である。

次に、本実施例により実際のデータを伝送する場合について示す。

ここでは、第６図において、情報シーケンス６００を送信する場合について考える。

伝送速度を最優先にした場合は、フレーム700がおくられ、暗号強度を最優先にした場合は、フレーム８００がおくられる。

フレームの構成は、開始フラグシーケンス610，フラグ制御シーケンス６２０，アドレスシーケンス６３０，制御シーケスン６４０，情報シーケンス６００，フレームチエツクシーケスンス６７０よりなつている。

まず、伝送速度を優先にした場合は、第３図に示した手順に従い、最初に開始フラグシーケンス６１０'01111110'が送られる。次に伝送速度が最大になるように、フラグシーケンス以外のフレームの部分に、ビット挿入箇所が最も少なくなるようなフラグ制御番号を選択する。ここでは、フラグ制御番号１が選択されたものとする。

次に、フラグ制御番号１に対応したフラグ制御シーケンス６２０'00000001'が伝送される。次に、アドレス・制御・情報・フレームチエツクの各シーケンスが伝送される。ここでは、フレーム制御番号１に対応した、フレーム挿入箇所が存在していないため、ビットパターンの挿入をすることなく伝送する。

次に、フラグ制御番号１に対応したフラグシーケンス'00000000'が終了フラグシーケンスとして伝送される。

以上により、伝送速度を優先した場合のフレーム７００が伝送される。

次に、暗号強度を優先した場合について示す。この場合も、第３図に示した手順に従い、最初に開始フラグシーケンス６１０'01111110'が送られる。次に暗号強度が最大となるようにフラグシーケンス以外の部分に、ビット挿入箇所が最も多くなるようなフラグ制御番号が選択する。ここでは、フラグ制御番号２５５が選択されたものとする。次にフラグ制御番号２５５に対応したフラグ制御シーケンス６２０'11111111'が伝送される。ただしここでは、フラグ制御番号２５５に対応した、フレーム挿入箇所が４箇所存在するため、各部分に、ビットパターン５００'1'がそれぞれ挿入されて伝送される。以上により暗号強度を優先した場合のフレーム８００が伝送される。

以上説明したごとく、伝送速度を優先した場合には、ビット挿入箇所が最小となるように、フラグ制御番号を選択し、送信側におけるビットパターンの挿入及び、受信側でのビットパターンの除去を最小限にして、処理時間を最小にすることにより、伝送速度を最大にすることができる。また、暗号強度を優先した場合は、ビット挿入箇所が最大となるようにフラグ制御番号を選ぶことにより、アドレス・制御・情報・フレームチエツクの各シーケンス内のビットパターン挿入箇所を最大とすることにより、データの傍受を困難ならしめ、暗号強度を最大にすることができる。

ここでは、具体的な例として、伝送速度を最優先にした場合と、暗号強度を最優先にした場合についてのみ示したが、本実施例によれば、最適な伝送速度，暗号強度を選ぶことにより柔軟な秘匿通信方式を実現することが可能である。

〔発明の効果〕

以上に説明したごとく本発明によれば、伝送する情報に合わせた最適な伝送速度及び、暗号強度を選択して情報の秘匿を行うことができ，通信回線の信頼性および、利用効率を向上させるという効果がある。

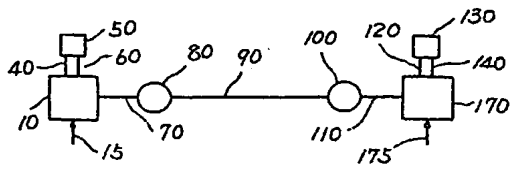
図面の簡単な説明

第１図は、本発明の一実施例である通信回線の構成を示した図、第２図は、本実施例によるフレームフオーマットを示した図、第３図は、本実施例における、送信器側の信号処理フローを示した

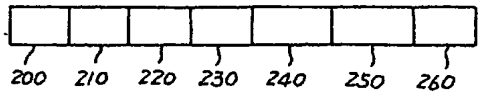
図、第４図は、本実施例における、受信器側の信号処理フローを示した図、第５図は、本実施例において、フレームシーケンスを秘匿するためのフラグ制御番号，フラグシーケンス，ビット挿入箇所，及びビットパターンの関係をあらわした表、第６図は、本実施例において、情報シーケンスを伝送速度を最優先にして送つた場合と、暗号強度を最優先にして送つた場合について示した図。

代理人　弁理士　小川勝男

第　1　図



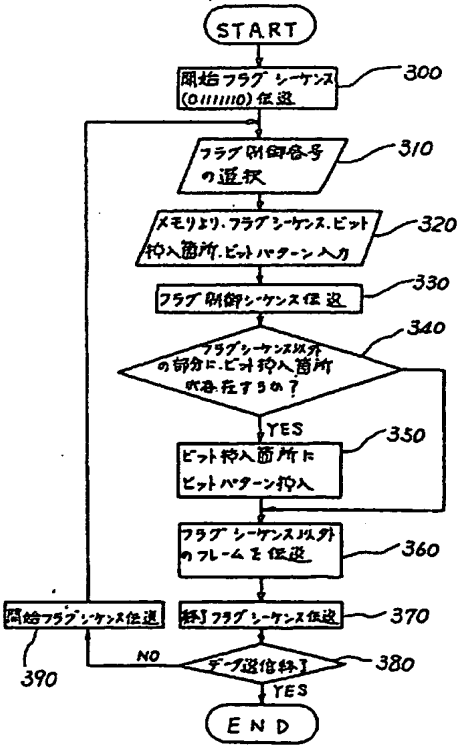
第　2　図



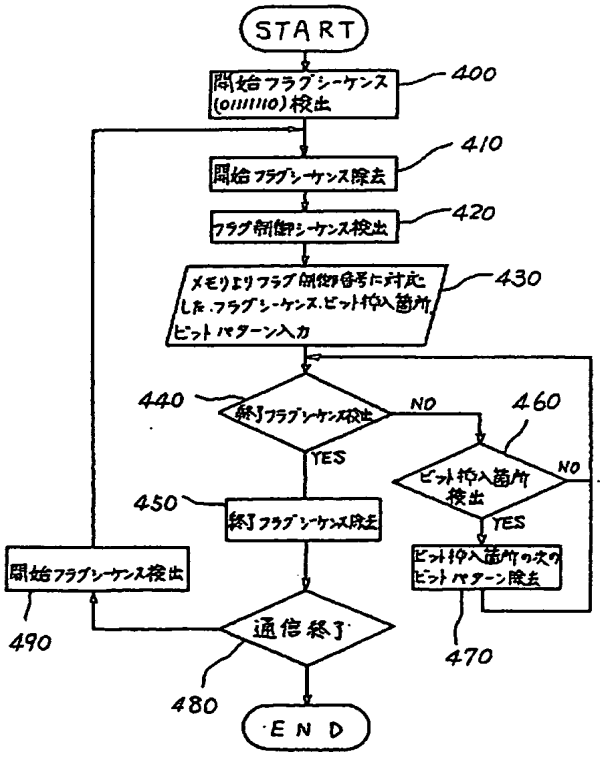
第　5　図

フラグ制御番号	フラグシーケンス	ビット挿入箇所	ビットパターン
1	00000000	00000000₂	1
2	11111111	1111111₂	0
3	11111110	111111₂	00
4	11111101	11111₂	000
5			
255	00000010	00000₂	1
256	00000001	000000₂	1

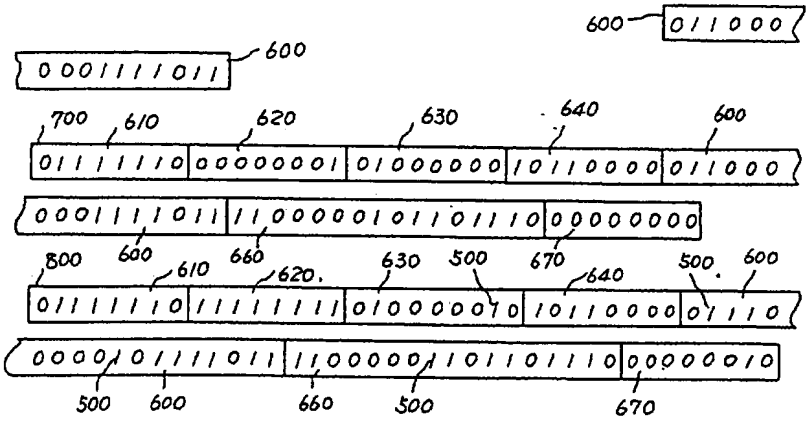
第　3　図



第　4　図



第 6 図


600
011000
600
0001111011
700
610
620
630
640
600
01111110
00000001
01000000
10110000
011000
0001111011
11000001011011110
00000000
800
600
610
660
620
630
500
670
640
500
600
01111110
11111111
01000010
10110000
01110
0000
01111011
11000001
01101110
00000010
500
600
660
500
670